HDE
Liberation of Technology

HDE Controller X

Self Monitoring Manual

HDE, Inc.

Please note that this user manual may be subjected to change due to product upgrades without any prior notice.

HDE and HDE Controller is a registered trademark of HDE, Inc.

All group names and product names listed in this manual are registered trademarks to each of the groups and products respectively.

This manual may only be copied by printing in PDF format. Any other forms of copying, transferring, loaning, adapting, translating, or public distribution of this manual is not allowed.

Reprinting or reproducing this manual without HDE's permission is strictly forbidden.

© 2011 HDE, Inc.

How to Read this Manual

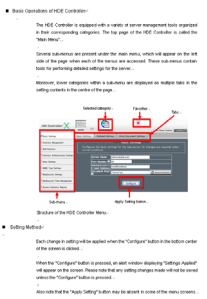
About this Manual

The “HDE Controller Installation Manual” provides users with instructions to installing OS and the HDE Controller (this Product) as well as steps for configuring the initial settings of the Product.

Annotations are provided for any matters requiring special attention and phrase supplements.

	Any matters which require special attention are marked with this "Alert" icon in bold frame.

	Contents which provide useful reference for using HDE Controller are marked with this "Hint" icon.



HDE Controller X

Self Monitoring

Summary

After setting up a server, it is necessary to monitor hardware resources, such as disk and memory, as well as processes executed on the server in order to maintain the server's stable operation. By monitoring server status, users can prevent various problems by detecting and copying with decrease in performance or resource before the server becomes unstable.

However, it requires a great amount of time and effort for the server administrator to be monitoring the server at all times, and may even lead to mistakes and problems due to human errors.

By utilizing the "Self-Monitoring" feature, the server administrator will be able to get a grasp of the server status, receive logs and warnings, and run pre-set scripts to auto-recover any damage without having to monitor the server manually at all times. Additionally, data on server status will be collected temporally and analyzed as a graph report. By accessing the "Graph Report" feature, the server administrators will be able to view the server status across a time period of their choice and set a threshold value and any actions corresponding to times when server activity exceeds the threshold value (sending warning mails, running scripts, etc) to detect any further abnormalities that may be present on the server at the present time or in the future.

Moreover, by accessing the "Server Status" menu, the administrator will be able to view the current server status and start or stop server services when necessary.

This section will introduce the methods of self-monitoring your server using HDE Controller.

■ Auto-Monitoring of Servers

● Setting up monitoring content and corresponding threshold values

The server will be able to self-monitor the following contents.

This section will provide an explanation for the definition of and how to set up a threshold value for each of the contents introduced. Please use this as a reference when setting up your own threshold values.

◇ (1) Disk and inode usage rates

Disk and inode usage capacities depend greatly on the file system you are using; however, when the disk and inode usage rate reaches 100%, users may not be able to save data, such as e-mails, on the hard disk, or may even cause the system to stop operating. Please make sure to configure your settings flexibly.

◇ (2) Actual memory usage rate

The usage rate of the actual memory, that is, the section of the physical memory which does not include buffer memory (buffer and cached). This value will be less than that of the memory which includes buffer memory. High usage rate of the actually memory may cause a decrease in the size of the buffer memory used by the system and lead to a decrease in performance. Please refer to the graph report and set your threshold value flexibly.

◇ (3) Physical memory usage rate

Usually, there will not be any problems even if this value is at 100%; however, the system performance may decrease if the difference between this value and the actual memory usage rate is small.

◇ (4) Swap usage rate

If your server considers a great deal about performance, it would be recommended to increase the capacity of your physical memory when using swap. Even if the server does not consider a great deal about performance, configure the threshold for this value flexibly as a 100% swap usage rate will cause your system to cease operation.

◇ (5) System usage rate

To be simply put, system load refers to the percent of CPU usage and is considered low if it is below 1.00 and high if it exceeds 1.00. Some delay may occur when executing certain processes when the system load is high.

Set your threshold value to around 2.0 if your system environment seldom executes heavy load processes. However, if your system environment often operates heavy load processes, it is recommended to set the threshold value as high as the system can handle such processes.

◇ (6) CPU usage rate

This value is displayed as an average CPU usage rate (excluding idle) up until the time when the system was late monitored. If this value is near 100% and the monitoring interval is set to 5 minutes, it means that the system has used the CPU close to its 100& capacity over a 5-minute time period. Such high CPU usage may imply insufficient CPU capacity or abnormalities in the executed processes. Please note that some process will require the use of CPU close to its 100% capacity even under normal circumstances. You may prevent receiving an alert for such processes by increasing the monitoring time interval.

◇ (7) Number of logged in users

System resources such as memory and CPU may be consumed by high number of user logins. At extreme cases, high number of logged in users will consume system resources which is required to provide the server services and may cause the system to cease operation. Please note that if this value is high even when you have not allowed login on your server, there may be problems with your server security and must be resolved swiftly to prevent unauthorized access.

It is recommended to set a minimum required threshold value for the number of logged in users unless you are using telnet or ssh for user login or are constantly monitoring your server. Please set an appropriate value in accordance with your working environment if you are using telnet or ssh.

◇ (8) Total number of processes

Process will consume a great amount of system resources such as memory and CPU. The consumed amount will increase as the number of executed processes increase and eventually cause the system to cease operation.

Please set an appropriate threshold value in accordance with your system status.

◇ (9) Number of processes running

The total number of processes running on the system. Administrators are not required to self-monitor this value unless necessary.

◇ (10) Number of sleep processes

The total number of processes waiting to be executed by the system. Administrators are not required to self-monitor this value unless necessary.

◇ (11) Number of paused processes

The number of processes paused by users. Paused processes will still consume system resource and a high number of such processes will lead to resource insufficiency.

Please set an appropriate threshold value in accordance with your working environment.

◇ (12) Number of zombie processes

Even though zombie processes themselves are not operable, they will still consume system resources when kept running and may disable users to start new processes.

Under normal circumstances, we recommend that you set this threshold value as 1; however, please set an appropriate threshold value in accordance with your working environment.

◇ (13) Number of optional processes

Some process types, such as crond, will be executed as a single process, whereas other processes, such as httpd, will be executed as multiple processes. Normal operations of the server may be effected if single processes are executed multiple times simultaneously or not executed all (service down), or if multiple processes are executed with excessive number of processes. Please configure an upper and/or lower limit for each process.

- Configuration Flow

◇ Send an E-mail under abnormal circumstances.

→ Configure a receiving mail address in the “Self Monitoring” – “Basic Settings” menu.

◇ Monitor server resources (memory, disk)

→ Configure threshold values and scripts to be executed upon abnormal circumstances in the “Self Monitoring” – “Resource Monitoring” menu.

◇ Monitor server load

→ Configure threshold values and scripts to be executed upon abnormal circumstances in the “Self-Monitoring” – “Performance Monitoring” menu.

◇ Monitor number of login users

→ Configure threshold values and scripts to be executed upon abnormal circumstances in the “Self-Monitoring” – “Login Monitoring” menu.

◇ Monitor total number of processes or zombie processes

→ Configure threshold values and scripts to be executed upon abnormal circumstances in the “Self-Monitoring” – “Process Monitoring” menu.

◇ Monitor total number of optional processes

→ Configure threshold values and scripts to be executed upon abnormal circumstances in the “Self-Monitoring” – “Optional Process Monitoring” menu.

◇ Display monitoring results in a time-based column graph

→ Initialize graph reports in the “Graph Reports” – “Initialization of Graph Reports” menu. You do not have to perform this step if the graph reports have already been initialized.

◇ Start self-monitoring process with the configured self-monitoring settings

→ Boot the self-monitoring and self-monitoring helper servers in the “Self Monitoring” – “Self Monitoring Service Status” menu.

◇ View the alert messages returned by self-monitoring

→ Click the corresponding graph reports for each of the contents you wish to view.

◇ Check the server status up to now and revise threshold values

→ Select the menu for the corresponding graph report in the “Graph Report” menu.

◇ Check the current server status

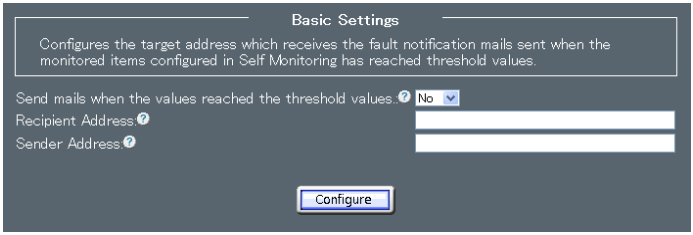
→ Please refer to the section on server monitoring by system administrator later in this manual.

Configure the threshold values and scripts on each configuration screen upon need.

Any changes made to the threshold value settings will be effective from the next monitoring cycle. You do not have to reboot any self-monitoring daemons or self-monitoring helper daemons in order to apply the setting changes.

1. Basic Settings

Configure whether or not to send an e-mail when the monitored values exceed each corresponding threshold values. By configuring alert mails, you will be able to get a grasp of the server status on your mobile phone or PDA.


Basic Settings
Configures the target address which receives the fault notification mails sent when the monitored items configured in Self Monitoring has reached threshold values.
Send mails when the values reached the threshold values.:
No
Recipient Address:
Sender Address:
Configure

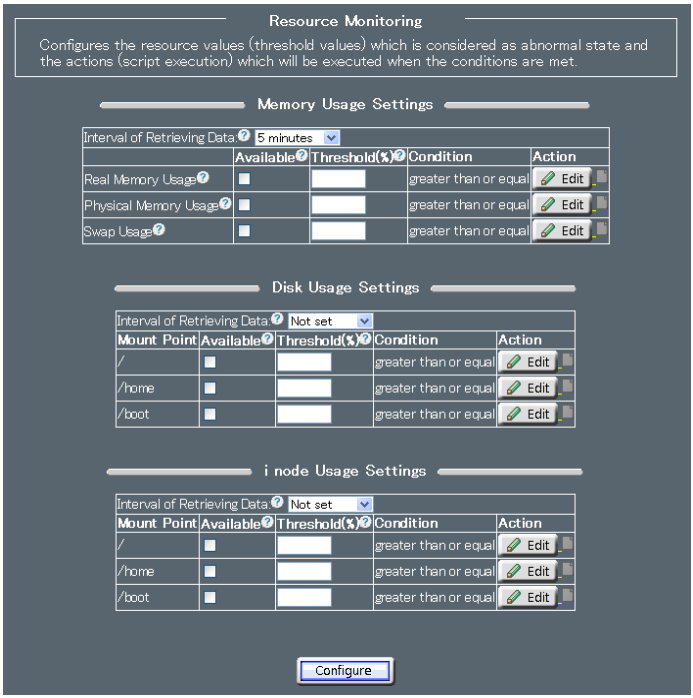
Click the “Configure” button to apply your settings.

Please note that if you enable e-mail notices, you will be receive an e-mail every time a monitored value exceeds its threshold value, and may end up with a large amount of e-mails depending on the server status.

2. Resource Monitoring

Configure whether or not to self-monitor and set threshold values to the following contents.

- Actual Memory Usage Rate
- Physical Memory Usage Rate
- swap Usage Rate
- Disk Usage Rate
- inode Usage Rate



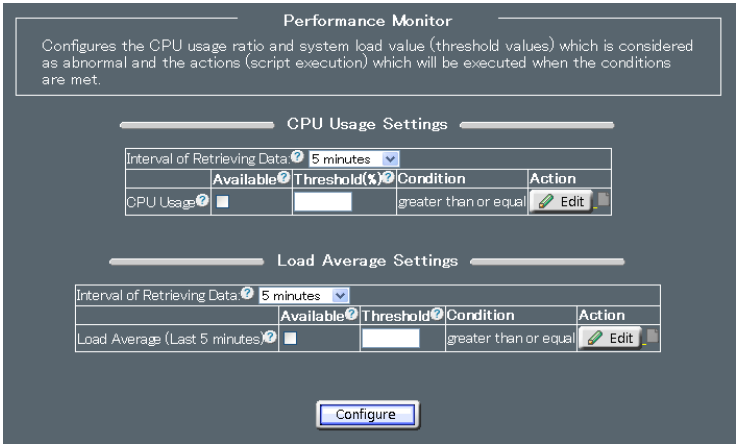
Configure whether or not to self-monitor and set threshold values for each of the contents. You may also configure the actions (scripts) of each of the contents by clicking the "Edit" button.

Click the "Configure" button to apply your settings.

3. Performance Monitoring

Configure whether or not to self-monitor and set threshold values to the following contents.

- CPU Usage Rate (average value obtained across monitoring interval)
- System Load (average value of the past 5 minutes)

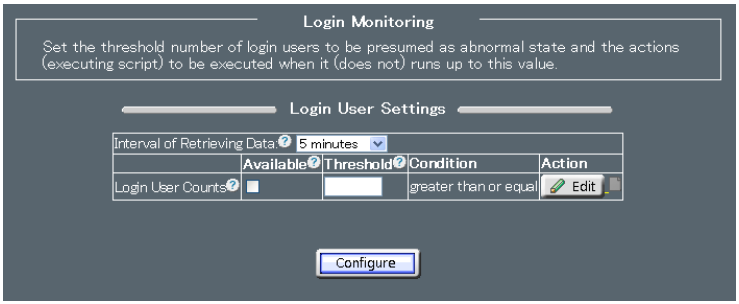


Configure whether or not to self-monitor and set threshold values for each of the contents. You may also configure the actions (scripts) of each of the contents by clicking the "Edit" button.

Click the "Configure" button to apply your settings.

4. Login Monitoring

Configure whether or not to self-monitor and set threshold values on user login counts.


Login Monitoring
Set the threshold number of login users to be presumed as abnormal state and the actions (executing script) to be executed when it (does not) runs up to this value.
Login User Settings
Interval of Retrieving Data:
5 minutes
Available
Threshold
Condition
Action
Login User Counts
greater than or equal
Edit
Configure

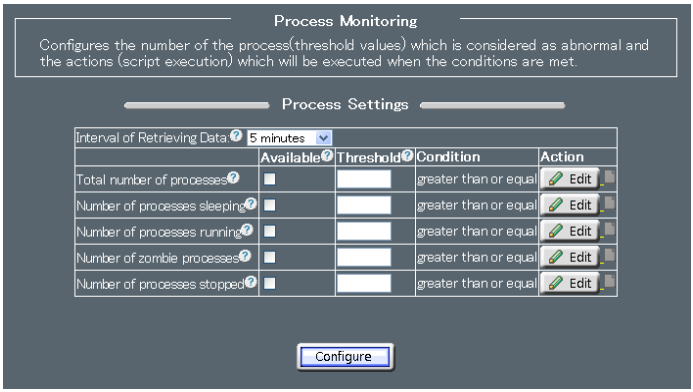
Configure whether or not to self-monitor and set threshold values for each of the contents. You may also configure the actions (scripts) of each of the contents by clicking the "Edit" button.

Click the "Configure" button to apply your settings.

5. Process Monitoring

Configure whether or not to self-monitor and set threshold values to the following contents.

- Total Number of Processes
- Number of Processes Running
- Number of Processes Sleeping
- Number of Zombie Processes
- Number of Processes Stopped



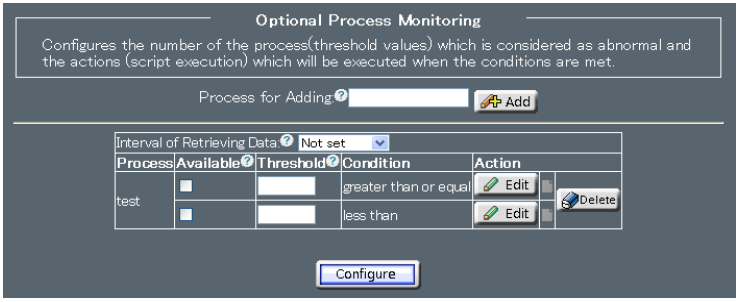
Configure whether or not to self-monitor and set threshold values for each of the contents. You may also configure the actions (scripts) of each of the contents by clicking the "Edit" button.

Click the "Configure" button to apply your settings.

6. Optional Process Monitoring

Add an optional process name and configure whether or not to self-monitor, and set threshold values to the process.

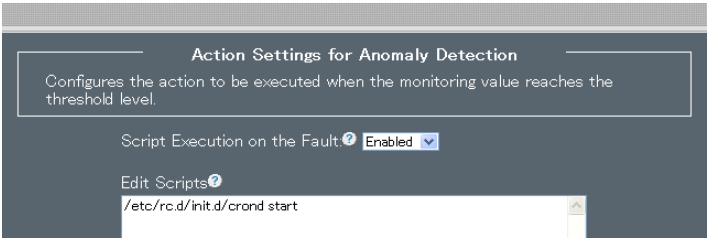
You may also set an upper and lower limit for each optional process.



For example, for processes, such as crond, involving the executing of a single process, you may set the upper limit to 2 and lower limit to 1 such that it would be regarded as abnormal by self-monitoring if the number of processes is over 2 or below 1(0). Additionally, you may also configure the following script and execute crond in case the number of processes drops below 1(0).

Script exampled used to execute crond:

/etc/rc.d/init.d/crond start


Action Settings for Anomaly Detection
Configures the action to be executed when the monitoring value reaches the threshold level.
Script Execution on the Fault:
Enabled
Edit Scripts
/etc/rc.d/init.d/crond start

Select the "Self Monitoring" - "Optional Process Monitoring" menu.

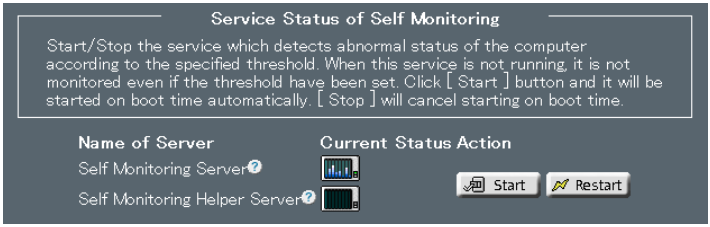
Enter the name of the process you wish to monitor in "Process for Adding" and click the "Add" button.

Configure whether or not to self-monitor and set threshold values for each of the contents. You may also configure the actions (scripts) of each of the contents by clicking the "Edit" button.

Click the "Configure" button to apply your settings.

7. Self Monitoring Service Status

Start or Stop services which send alerts to the computer when configured threshold values are compromised. Please note that if you do not start this service, self-monitoring will not be performed even when the threshold values are configured. Once the "Start" button is pressed, the self-monitoring service will start automatically upon your next system boot. You may cancel the auto-start of self-monitoring upon boot-up by clicking the "Stop" button.

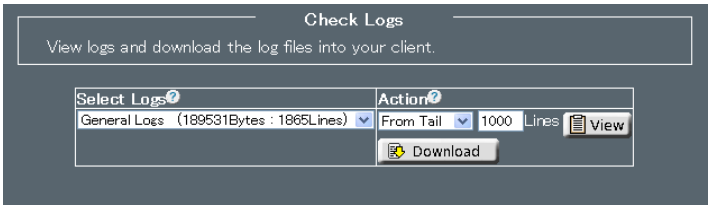

Service Status of Self Monitoring
Start/Stop the service which detects abnormal status of the computer according to the specified threshold. When this service is not running, it is not monitored even if the threshold have been set. Click [Start] button and it will be started on boot time automatically. [Stop] will cancel starting on boot time.
Name of Server
Current Status
Action
Self Monitoring Server
Self Monitoring Helper Server
Start
Restart

Click the “Start” or the “Stop” button.

8. View Alerts

An alert log will be created when configured threshold values are compromised. You can check this log file to find out the cause of the compromise and improve/maintain server operation stability.

Select the "Log Management" – “Check Logs" menu.



Select the "Alert logs for Self Monitoring" and click the "View" button to view the alert logs created by self-monitoring.

HDE Controller PRO / LG User Manual

April 30, 2011 1st Ed. 10.0-001

HDE, Inc.

16-28, Nanpeidaicho, Shibuya, TOKYO, 150-0036 JAPAN